Capitolo 8

Il teorema di Ruffini-Abel

8.1 Paolo Ruffini e la risolubilità delle equazioni algebriche

L'ultima parte delle *Réflexions* si apre con l'esposizione degli esiti dell'analisi dei metodi di risoluzione per equazioni di grado superiore al quarto, per le quali il problema della risolubilità algebrica era ancora aperto.

Si è potuto constatare, grazie all'analisi dei principali metodi noti di risoluzione delle equazioni che abbiamo appena esposto, che tutti questi metodi si riducono ad uno stesso principio generale, quello di trovare delle funzioni delle radici dell'equazione proposta tali: 1° che l'equazione o le equazioni da cui saranno ottenute, cioè a dire di cui saranno le radici (equazioni che vengono comunemente dette ridotte) abbiano un grado minore di quello dell'equazione proposta o siano almeno scomponibili in altre equazioni di un grado inferiore della proposta; 2° che dalle ridotte si possano dedurre facilmente i valori delle radici cercate.

L'arte di risolvere le equazioni consiste dunque nello scoprire delle funzioni delle radici che abbiano le proprietà appena enunciate; ma è sempre possibile trovare tali funzioni per le equazioni di grado qualsiasi, cioè per un numero di radici arbitrario? Questo è un punto su cui sembra essere molto difficile di potersi pronunciare in generale.[1] ([1], §86, p.355)

[1] On a du voir par l'analyse que nous venons de donner des principales methodes connues pour la résolution des équations, que ces méthodes se réduisent otutes à un même principe général, savoir à trouver des fonctions des racines de l'équation proposée, lesquelles soient telles: 1° que l'équation ou les équations par lesquelles elles seront données, c'est-à-dire dont elles sont racines (équations qu'on nomme communément les réduites), se trouvent d'un degré moindre que celui de la proposée, ou soient au moins décomposables en d'autres équations 'un degré moindre que celui-là; 2° que l'on puisse en déduire aisément les valeurs des racines cherchées.

L'art de résoudre les équations consiste donc à découvrir des fonctions des racines, qui aient les propriétés que nous venons d'énoncer; mais est-il toujours possible de trouver de telles fonctions, pour les équations d'un dégre quelconque, c'est-à-dire pour tel nombre de racines qu'on voudra? C'est sur qoui il parait très-difficile de pouvoir prononcer en général.

Sul finire delle *Réflexions* Lagrange esprime la ferma convinzione di aver svelato i principi autentici che si celano dietro i metodi di risoluzione delle equazioni algebriche e che sono alla base del loro successo per equazioni di grado non superiore al quarto ma egualmente è consapevole che la risolubilità algebrica di equazioni di grado superiore per questa via è ancora lontana dall'essere ottenuta:

Ecco, se non mi sbaglio, gli autentici principi della risoluzione delle equazioni e l'analisi più appropriata a svelarli; il tutto si riduce, come si è visto, ad una sorta di calcolo di combinazioni, tramite il quale si trovano a priori i risultati che uno può aspettarsi. Sarebbe opportuno farne l'applicazione ad equazioni di quinto grado e di gradi superiori la cui soluzione è ad oggi sconosciuta; tuttavia questa applicazione richiede un numero troppo grande di ricerche e di combinazioni, la cui riuscita è ancora molto dubbia perché possa dedicarmi attualmente a questo lavoro; mi auguro tuttavia di potervi ritornare in altri tempi e mi accontenterò per ora di aver qui gettato le basi di una teoria che mi sembra nuova e generale.[2] ([1], §109, p. 403).

Con Lagrange, Vandermonde e Waring, le cui *Meditationes Algebraicae* contengono alcuni dei risultati ottenuti dagli altri due matematici, si chiude un periodo nella storia delle equazioni algebriche e si gettano le premesse di una nuova stagione di sviluppi. Non è un caso se i lavori di questi tre matematici, apparsi o comunque inviati per la pubblicazione all'incirca nello stesso periodo, gli anni attorno al 1770, siano seguiti da quasi trent'anni di stasi sul problema della risolubilità algebrica delle equazioni. Alla fine del XVIII secolo nasce una nuova fase che condurrà ad un esito per certi aspetti sorprendente: l'impossibilità di ottenere in generale una soluzione algebrica per equazioni di grado superiore al quarto. In verità, nel 1799 Gauss, nella Dissertazione [2] studiata al Cap. 6, si esprimeva in termini piuttosto scettici circa la possibilità di ottenere una formula risolutiva per equazioni di grado qualunque:

Dopo tante fatiche di molti geometri rimane solo una minima speranza di poter pervenire un giorno alla risoluzione generale delle equazioni algebriche ed appare sempre più verosimile che una tale risoluzione sia impossibile e contraddittoria. Ciò non deve sembrare paradossale in quanto ciò che abitualmente viene detta soluzione di un'equazione altro non è che la riduzione dell'equazione ad equazioni pure. Ora in tutto questo non si insegna a risolvere le equazioni pure, ma se ne presuppone la soluzione e, se si esprime con $\sqrt[m]{H}$ *la radice dell'equazione* $x^m = H$*, non la si risolve affatto e non si fa altro di quanto si farebbe escogitando un qualche segno per indicare la radice dell'equazione* $x^n + Ax^{n-1} + ... = 0$ *e si ponesse questo segno uguale alla radice. È vero che le equazioni pure sono di gran lunga superiori alle altre sia per la facilità*

[2] Voilà, si je ne me trompe, les vrais principes de la résolution des équations et l'analyse la plus propre à y conduire; tout se réduit, comme on voit, à une espèce de calcul des combinaisons, par lequel on trouve à priori les résultats auxquels on doit s'attendre. Il serait à propos d'en faire l'application aux équations du cinquième degré et des degrés superieur, dont la résolution est jusqu'à présent inconnue; mais cette application demande un trop grand nombre de recherches et de combinaisons, dont le succès est encore d'ailleurs fort douteux, pour que nous puissions quant à present nous livrer à ce travail; nous espérons cependant pouvoir y revenir dans un autre temps, et nous nous contenterons ici d'avoir posé les fondaments d'une théorie qui nous parait nouvelle et générale.

con cui si trovano le loro radici per approssimazione, sia per il legame elegante che esiste tra le radici stesse e pertanto non si deve in alcun modo disprezzare che gli analisti abbiano loro attribuito un simbolo specifico; tuttavia dal fatto di aver raggruppato tale simbolo con quelli delle operazioni aritmetiche di somma, sottrazione, moltiplicazione, divisione ed elevamento a potenza sotto il nome di espressioni analitiche, non segue affatto che per mezzo di questi simboli si possa esprimere la radice di una equazione qualsiasi. Ovvero, per farla breve, si presuppone senza una motivazione sufficiente che la soluzione di un'equazione arbitraria si possa ridurre alla soluzione di equazioni pure. Non sarà forse difficile dimostrare rigorosamente tale impossibilità già per le equazioni di quinto grado, sulla qual cosa proporrò con più particolari le mie argomentazioni in un altro luogo[3]([2], p.17)

Nel medesimo anno in cui il giovane Gauss esprimeva con queste parole il proprio scetticismo, Paolo Ruffini, medico e matematico italiano attivo a Modena, pubblicava una monografia che, fin dal titolo, prendeva posizione netta sulla questione affermando di aver dimostrato l'impossibilità di risolvere in generale un'equazione di grado superiore al quarto: *Teoria generale delle Equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto* [3]. Ruffini dichiara apertamente l'importanza che l'opera di Lagrange sulle equazioni algebriche ha avuto sui risultati contenuti nella *Teoria generale* al punto da indicare come titolo di merito della propria opera quello di avere radunato ed organizzato molto di quanto Lagrange aveva scritto sull'argomento in diverse memorie. La dimostrazione del teorema fu, è facile immaginarlo, bersagliata da critiche, alcune benevole altre meno, cui Ruffini rispose con nuove versioni della dimostrazione tese a chiarirne e semplificarne l'impianto, fino alla versione finale, licenziata nel 1813. Come vedremo, la dimostrazione finale di Ruffini contiene un'affermazione che occorreva giustificare e questa lacuna venne colmata nel 1826 dal grande matematico norvegese Niels-Henrik Abel (1802-1829) con un lavoro [4] che parte da premesse diverse rispetto a quelle di Ruffini e che pure, su un punto non vitale per la validità

[3]Post tot tantorum geometrarum labores perexiguam spem superesse, ad resolutionem generalem aequationum algebraicarum unquam perveniendi, ita ut magis magisque verisimile fiat, talem resolutionem omnino esse impossibilem et contradictoriam. Hoc eo minus paradoxum videri debet, quum id quod vulgo resolutio aequationis dicitur, proprie nihil aliud sit quam ipsius reductio ad aequationes puras. Nam aequationum purarum solution hinc non docetur sed supponitur, et si radicem aequationis $x^m = H$ per $\sqrt[m]{H}$ exprimis, illam neutiquam solvisti neque plus fecisti, quam si ad denotandam radicem aequationis $x^n + Ax^{n-1} + ... = 0$ signum aliquod excogitares, radicemque hinc aequalem poneres. Verum est aequationes puras propter facilitarum ipsarum radices per approximationem inveniendi, et propter nexum elegantem, quem omnes radices inter se habent, prae omnibus reliquis multum praestare, adeoque neutiquam vituperandum esse, quod analystae harum radicis per signum peculiare denotaverunt; attamen, ex eo, quod hoc signum perinde ut signa arithmetica additionis, subtractionis, multiplicationis, divisionis et evectionis ad dignitatem sub nomine expressionum analyticarum complexi sunt, minime sequitur, cuiusvis aequationis radicem per illas exhiberi posse. Seu, missis verbis, sine ratione sufficienti supponitur, cuiusvis aequationis solutionem ad solutionem aequationum purarum reduci posse. Forsan non ita difficile foret, impossibilitatem iam pro quinto gradu omni rigore demonstrare, de qua re alio loco disquisitiones meas fusius proponam.

della dimostrazione, contiene un errore messo in evidenza da William Rowan Hamilton (1805-1865).

Vedremo in questo capitolo lo schema generale dell'ultima dimostrazione del teorema di impossibilità data da Ruffini dopo un breve cenno alle diverse versioni che nel giro di quindici anni egli pubblicò. Metteremo in evidenza il punto debole dell'argomento di Ruffini ed enunceremo il lemma grazie a cui Abel ottenne una dimostrazione completa del teorema.

8.2 Cronaca delle dimostrazioni di Ruffini

Come accennato in precedenza, la prima dimostrazione del teorema di impossibilità si trova nella *Teoria Generale delle Equazioni*, a partire dal Capitolo XIII. Dapprima Ruffini classifica le permutazioni, sviluppando e sistematizzando quel *calcul des combinaisons* che Lagrange aveva abbozzato nelle *Réflexions*. Con Lagrange e Cauchy, Ruffini può essere considerato uno dei pionieri della teoria dei gruppi o, meglio, del gruppo delle permutazioni che veniva e sarebbe stato per molto tempo chiamato gruppo delle sostituzioni, riservando invece il termine di permutazione a ciò che oggi viene detto arrangiamento di un insieme di n oggetti. La prima dimostrazione di Ruffini non è sempre chiara, come egli stesso ebbe a notare poco dopo, anche per la mancanza di una apposita notazione per le permutazioni che rende necessaria una descrizione caso per caso che appesantisce la lettura del lavoro. Heinrich Burkhardt, che fu uno dei primi a sottolineare l'importanza dell'opera di Ruffini nello sviluppo del concetto di gruppo [5], sollevò una serie di obiezioni che potevano essere mosse alla dimostrazione del 1799, come l'aver tacitamente assunti come validi diversi teoremi di Lagrange che, al contrario, erano ancora privi di una solida dimostrazione o l'aver dato per valida la dimostrazione del teorema fondamentale dell'algebra proposta da Lagrange. La mancanza di un'adeguata notazione obbligò Ruffini ad una lunga descrizione di casi possibili che non sempre è completa; manca inoltre una solida dimostrazione di alcuni punti tecnici importanti per l'impianto del teorema. Mentre nelle versioni successive tutte queste imperfezioni poterono essere superate o almeno ritenute errori veniali, una mancanza sostanziale presente ancora nell'ultima dimostrazione di Ruffini è l'aver considerato come punto di paertenza solo funzioni razionali delle radici e non anche irrazionali, funzioni queste ultime che Leopold Kronecker (1823-1891) chiamerà *irrazionalità accessorie*. Questo fatto, che Ruffini pone come ipotesi, è invece il cuore del Lemma di Abel la cui dimostrazione è necessaria per rendere completo l'argomento di Ruffini.

Nel 1801 Ruffini presentò alla Società Italiana delle Scienze una memoria [6], pubblicata l'anno successivo, in cui si poneva la domanda di individuare in quali casi la risoluzione di un'equazione di grado qualsiasi fosse ottenibile grazie alla sua riduzione ad un'altra equazione di grado inferiore. Nel 1803, sulla stessa rivista, venne publicata una lettera di Pietro Abbati, conte Marescotti (1768-1842), a Ruffini nella quale egli intendeva semplificare alcuni punti della dimostrazione di Ruffini del 1799. In particolare, in quest'opera Abbati mostra

il teorema già enunciato da Lagrange e ripreso da Ruffini ma, in entrambi i casi senza dimostrazione, che il numero di valori formalmente distinti che una funzione di n elementi può assumere è un divisore di $n!$. Le osservazioni di Abbati saranno incorporate da Ruffini in una memoria [7] pubblicata nel 1803 che, sostanzialmente, ha come unico difetto il mancato riferimento alle irrazionalità accessorie. Nel 1804 Gian-Francesco Malfatti (1731-1807) pubblicò un articolo [8] in cui esponeva le proprie riserve circa l'argomento di Ruffini. In particolare egli costruì un esempio di equazione di quinto grado la cui risolvente di sesto grado possiede una radice razionale e si domandava in qual modo fosse possibile escludere che una tale eventualità non si presentasse nelle risolventi di un'equazione di quinto grado generica. A questa memoria, il cui punto saliente è proprio la costruzione della risolvente di sesto grado, nota oggi come *risolvente di Malfatti*, Ruffini rispose nel 1805 [9] per poi dedicarsi ancora al problema nel 1806 con un lavoro non molto felice [10] in cui affrontava la possibilità di risolvere le equazioni di grado superiore al quarto con metodi trascendenti. Infine giungiamo all'ultima redazione, quella del 1813 [11] che è certo la più sintetica e che, presa singolarmente, lascia in ombra il grande lavoro svolto da Ruffini per gettare le basi della teoria dei gruppi.

8.3 Schema della dimostrazione del 1813

Cerchiamo di capire come Ruffini intende procedere discutendo un esempio particolare. Una formula risolutiva algebrica per l'equazione

$$x^m + ax^{m-1} + bx^{m-2} + \cdots + u = 0 \tag{8.1}$$

consiste nel trovare una funzione $F(x_1, x_2, \cdots, x_n)$ delle radici di (8.1) che ne dipenda in modo simmetrico, in modo da poter essere espressa in termini dei coefficienti di (8.1): $F(x_1, x_2, \cdots, x_n) = f(a, b, c, \cdots u)$ e grazie alla quale sia possibile esprimere *tutte* le radici di (8.1). L'ambiguità in una tale formula, già evidenziata da Vandermonde, risiede in questo: se

$$x_1 = F^*(x_1, x_2, \cdots, x_n),$$

dove F^* indica una determinazione particolare della F, allora permutando in ambo i membri x_1 ed x_2, si deve anche avere

$$x_2 = F^*(x_2, x_1, \cdots, x_n).$$

Ad esempio questa situazione si presenta nella formula risolutiva delle equazioni di secondo grado che, detta $\alpha = \pm 1$ una radice quadrata dell'unità, si può scrivere come

$$x = \frac{-b + \alpha\sqrt{b^2 - 4c}}{2},$$

scelto $\alpha = +1$ e ricordando che $b = -(x_1 + x_2)$, $c = x_1 x_2$ e che il radicando va considerato in senso aritmetico, si ottiene

$$x_1 = \frac{(x_1 + x_2) + \sqrt{(x_1 + x_2)^2 - 4x_1x_2}}{2} = F^*(x_1, x_2).$$

D'altra parte, se si permutano tra loro x_1 ed x_2 ad ambo i membri, e si considera ancora il radicale in senso aritmetico, si ha

$$x_2 = F^*(x_2, x_1) :$$

tutti gli argomenti di Ruffini vogliono dimostrare come una formula risolutiva di questo tipo sia contraddittoria quando $m > 4$.

La dimostrazione di Ruffini poggia su alcuni risultati preliminari, alcuni dei quali già presenti nella prima versione del 1799.

• Se

$$z^n + mz^{n-1} + nz^{n-2} + \cdots + v = 0 \tag{8.2}$$

è l'equazione trasformata di (8.1), allora le radici z_k di (8.2) saranno funzioni di quelle di (8.1):

$$z_k = f(x_1, x_2, \cdots, x_n). \tag{8.3}$$

• Per descrivere l'azione di una permutazione su un insieme di argomenti Ruffini, a partire dalla *Teoria Generale*, aveva proposto diversi esempi didatticamente efficaci. Così, ad esempio, se

$$f(x_1, x_2, x_3) = \frac{x_1^1}{x_2} + \frac{3x_2x_3^2}{x_1} + ax_2$$

si ha anche

$$f(x_2, x_1, x_3) = \frac{x_2^2}{x_1} + \frac{3x_1x_3^2}{x_2} + ax_1.$$

• Se i coefficienti m, n, ..., v della (8.2) sono ciascuno funzione razionale dei coefficienti a, b,...., u della (8.1), allora permutando tra loro le $x_1, x_2, \cdots, x_n$ nella (8.3) si otterrà sempre una radice di (8.2) ed il numero di valori distinti assunto da f è un sottomultiplo di $n!$.

• Se la funzione (8.3) è di forma tale che uno dei suoi valori è inalterato per effetto di una permutazione che coinvolge le radici che figurano in certe posizioni, iterando la permutazione, la (8.3) non cambia valore. Consideriamo la funzione

$$f(x_1, x_2, x_3, x_4) = \sqrt{x_1x_2^2} + \sqrt{x_2x_3^2} + \sqrt{x_3x_1^2} - x_4$$

che rimane inalterata sotto l'azione della permutazione

$$\sigma = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_3 & x_1 & x_4 \end{pmatrix} :$$

essa non cambierà valore anche sotto l'azione di

$$\sigma^2 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_3 & x_1 & x_2 & x_4 \end{pmatrix}$$

e di $\sigma^3 = \mathrm{id}$, dove id è l'identità. In altre parole

$$f(x_1, x_2, x_3, x_4) = f(x_2, x_3, x_1, x_4) = f(x_3, x_1, x_2, x_4).$$

Allo stesso modo, se si considera l'azione di σ sull'arrangiamento (x_4, x_2, x_3, x_1) si otterrà

$$f(x_4, x_2, x_3, x_1) = f(x_2, x_3, x_4, x_1) = f(x_3, x_4, x_2, x_1).$$

Come conseguenza, se applicando p volte su una certa funzione $f(x_1, x_2, \cdots, x_n)$ una certa permutazione σ, rispetto alla quale f è invariante, tale che $\sigma^p = \mathrm{id}$, allora la f assumerà tutti i suoi valori con molteplicità p.

Entriamo ora più in dettaglio nel ragionamento di Ruffini servendoci della presentazione di Maracchia [12]. Punto chiave della dimostrazione è l'esame di espressioni del tipo

$$y^p = \Pi := F(x_1, x_2, \cdots, x_n) \tag{8.4}$$

dove $\{x_1, \cdots, x_n\}$ sono le radici di (8.1). Denotiamo con $y_1 = f(x_1, x_2, \cdots, x_n)$ una soluzione di (8.4) che si potrà sempre esprimere come

$$y_1 = \alpha \sqrt[p]{\Pi}, \qquad \text{con} \qquad \alpha^p = 1.$$

Ruffini dimostra il seguente

Teorema I. Se Π è invariante sotto l'azione di qualche permutazione σ delle $\{x_1, \cdots, x_n\}$, allora operando con la stessa permutazione su f si ottiene un'altra radice di (8.4).

Dim. Consideriamo la permutazione

$$\sigma = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & \cdots \\ x_2 & x_3 & x_4 & x_5 & x_1 & \cdots \end{pmatrix} \tag{8.5}$$

e supponiamo che lasci invariata Π. Ciò significa che

$$\Pi = F(x_1, x_2, x_3, x_4, x_5, \cdots) = F(x_2, x_3, x_4, x_5, x_1, \cdots) = F(x_3, x_4, x_5, x_1, x_2, \cdots)$$
$$F(x_4, x_5, x_1, x_2, x_3, \cdots) = F(x_5, x_1, x_2, x_3, x_4, \cdots)$$

ed operando con σ su f si otterranno i valori

$$\begin{aligned} y_1 &= f(x_1, x_2, x_3, x_4, x_5, \cdots) \\ y_2 &= f(x_2, x_3, x_4, x_5, x_1, \cdots) \\ y_3 &= f(x_3, x_4, x_5, x_1, x_2, \cdots) \\ y_4 &= f(x_4, x_5, x_1, x_2, x_3, \cdots) \\ y_5 &= f(x_5, x_1, x_2, x_3, x_4, \cdots). \end{aligned}$$

Siccome y_1 risolve (8.4), allora

$$[f(x_1, x_2, x_3, x_4, x_5, \cdots)]^p = F(x_1, x_2, x_3, x_4, x_5, \cdots) = \Pi$$

e questa uguaglianza deve conservarsi anche operando con σ su ambo i membri. Così facendo però il membro di destra non varia per ipotesi mentre a sinistra y_1 viene mutata in uno degli altri valori $y_2, \cdots, y_5$ che dunque sono anch'esse radici di (8.4).

In particolare, dovrà esistere un'altra radice p-esima dell'unità γ tale che

$$y_2 = \gamma \sqrt[p]{\Pi}$$

oltre ad avere $y_1 = \alpha \sqrt[p]{\Pi}$. Dunque

$$\frac{y_2}{y_1} = \frac{\gamma}{\alpha}$$

ma siccome $\alpha^p = \gamma^p = 1$, anche $\beta := \frac{\gamma}{\alpha}$ è una radice p-esima dell'unità e possiamo così concludere che

$$y_2 = \beta y_1, \qquad \text{con} \qquad \beta^p = 1.$$

Se ora agiamo ripetutamente con σ su ambo i membri di questa uguaglianza otteniamo

$$y_2 = \beta y_1, \quad y_3 = \beta y_2, \quad y_4 = \beta y_3, \quad y_5 = \beta y_4, \quad y_1 = \beta y_5$$

cioè

$$y_1 = \beta y_5 = \beta^2 y_4 = \beta^3 y_3 = \beta^4 y_2 = \beta^5 y_1$$

che impone che β sia una radice quinta dell'unità:

$$\beta^5 = 1. \tag{8.6}$$

Teorema II. Si supponga che Π sia anche invariante sotto l'azione della permutazione

$$\sigma_a := \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & \cdots \\ x_2 & x_3 & x_1 & x_4 & x_5 & \cdots \end{pmatrix} \tag{8.7}$$

che dunque agisce solo sulle tre radici x_1, x_2, x_3. Allora, i corrispondenti valori di y sono uguali tra loro.
Dim. Per ipotesi si ha

$$\Pi = F(x_1, x_2, x_3, x_4, x_5, \cdots) = F(x_2, x_3, x_1, x_4, x_5, \cdots) = F(x_3, x_1, x_2, x_4, x_5, \cdots).$$

Siano ora

$$y_1 = f(x_1, x_2, x_3, x_4, x_5, \cdots) \quad y_a = f(x_2, x_3, x_1, x_4, x_5, \cdots) \quad y_{a+1} = f(x_3, x_1, x_2, x_4, x_5, \cdots)$$

i corrispondenti valori di y: occorre mostrare che $y_1 = y_a = y_{a+1}$. Infatti, ripetendo l'analisi utilizzata per dimostrare il precedente teorema si ottiene l'esistenza di una radice p-esima dell'unità γ tale che

$$y_a = \gamma y_1, \qquad y_{a+1} = \gamma y_a \qquad \text{e} \qquad y_1 = \gamma y_{a+1}.$$

e che dunque deve verificare

$$y_1 = \gamma y_{a+1} = \gamma^2 y_a = \gamma^3 y_1$$

sicché deve essere una radice *terza* dell'unità:

$$\gamma^3 = 1.$$

Permutiamo ora ciclicamente gli argomenti di y_a, ottenendo

$$y_a = f(x_2, x_3, x_1, x_4, x_5, \cdots) \mapsto y_b = f(x_3, x_1, x_4, x_5, x_2, \cdots)$$

ed osserviamo che la relazione tra y_b ed y_a è la stessa di quella tra y_2 ed y_1. Consideriamo la permutazione σ_b data da

$$\sigma_b := \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & \cdots \\ x_3 & x_1 & x_4 & x_5 & x_2 & \cdots \end{pmatrix} = \sigma_a \sigma \tag{8.8}$$

ed applichiamola ripetutamente ad y_1:

$$\begin{aligned} y_1 &= f(x_1, x_2, x_3, x_4, x_5, \cdots) \\ y_b &= f(x_3, x_1, x_4, x_5, x_2, \cdots) \\ y_{b+1} &= f(x_4, x_3, x_5, x_2, x_1, \cdots) \\ y_{b+2} &= f(x_5, x_4, x_2, x_1, x_3, \cdots) \\ y_{b+3} &= f(x_2, x_5, x_1, x_3, x_4, \cdots) \\ y_{b+4} &= f(x_1, x_2, x_3, x_4, x_5, \cdots) = y_1. \end{aligned}$$

Siccome y_b ed y_a sono legate tra loro dalla stessa relazione che intercorre tra y_2 ed y_1 del Teorema I, sappiamo che esiste una radice quinta dell'unità β tale che

$$y_b = \beta y_a$$

e dunque

$$y_b = \beta\gamma y_1.$$

Ripetendo l'analisi del Teorema I sui valori $y_1, y_b, \cdots y_{b+3}$ ricaviamo

$$y_b = \beta\gamma y_1 \quad y_{b+1} = \beta\gamma y_b \quad y_{b+2} = \beta\gamma y_{b+1} \quad y_{b+3} = \beta\gamma y_{b+2} \quad y_1 = \beta\gamma y_{b+3}$$

cosicché si ha

$$y_1 = (\beta\gamma)^5 y_1$$

per cui anche $\beta\gamma$ è una radice quinta dell'unità. Poiché però si ha $\beta^5 = \gamma^3 = 1$ si deve avere $\gamma^2 = 1$ e dunque $\gamma = 1$, visto che il valore -1 non è una radice terza dell'unità. È dunque vero che $y_1 = y_a = y_{a+1}$.

In modo del tutto analogo si dimostra il

Teorema III. Si supponga che valgano ancora le ipotesi del Teorema I e che inoltre Π sia invariante sotto l'azione della permutazione

$$\sigma_c := \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & \cdots \\ x_1 & x_2 & x_4 & x_5 & x_3 & \cdots \end{pmatrix} : \tag{8.9}$$

allora si ha che

$$y_1 = f(x_1, x_2, x_3, x_4, x_5, \cdots), \quad y_c = f(x_1, x_2, x_4, x_5, x_3, \cdots) \quad y_{c+1} = f(x_1, x_2, x_5, x_3, x_4, \cdots)$$

sono uguali tra loro.

Teorema IV. Supponiamo ora che Π sia invariante rispetto a tutte le permutazioni considerate nei Teoremi I-III. Allora

$$y_1 = y_2 = y_3 = y_4 = y_5 = y_a = y_{a+1} = y_c = y_{c+1}.$$

Dim. Se valgono i Teoremi II e III sappiamo che $y_1 = y_a = y_{a+1}$ ed $y_1 = y_c = y_{c+1}$. Ora, se applichiamo σ_c ad $y_a = y_1$ otteniamo

$$y_a = f(x_2, x_3, x_1, x_4, x_5, \cdots) \mapsto f(x_2, x_3, x_4, x_5, x_1, \cdots) = y_2$$

e poiché l'applicazione di σ_c ad $y_a = y_1$ non altera il valore di y_1, essa non altera il valore neppure di y_a sicché

$$y_1 = y_2,$$

che chiude la dimostrazione.

Osservazione. È istruttivo far vedere, come in [12], perché questo argomento *non* è conclusivo se $n = 4$. Infatti, se si considerano le permutazioni

$$\tau := \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & \cdots \\ x_2 & x_3 & x_4 & x_1 & \cdots \end{pmatrix}, \quad \tau_a := \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & \cdots \\ x_2 & x_3 & x_1 & x_4 & \cdots \end{pmatrix}$$

e

$$\tau_c := \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & \cdots \\ x_1 & x_3 & x_4 & x_2 & \cdots \end{pmatrix},$$

rispetto alle quali si ha invarianza di Π si può ancora dimostrare, analogamente a quanto visto prima, si ha che

$$\begin{aligned} &y_1 = f(x_1, x_2, x_3, x_4, \cdots) = y_a = f(x_2, x_3, x_1, x_4, \cdots) = y_{a+1} = f(x_3, x_1, x_2, x_4, \cdots) \\ &= y_c = f(x_1, x_3, x_4, x_2, \cdots) = y_{c+1} = f(x_1, x_4, x_2, x_3, \cdots). \end{aligned}$$

Se ora si applica τ_c ad y_a si ottiene $f(x_2, x_1, x_4, x_3) \neq y_2 = f(x_2, x_3, x_4, x_1)$ e dunque non si possono trarre le conseguenze del Teorema IV.

Completata questa minuziosa parte combinatoria, Ruffini può ora dimostrare il teorema di impossibilità:

Teorema È impossibile risolvere algebricamente un'equazione generale come (8.1) quando $n > 4$.

Dim. L'ipotetica formula risolutiva deve contenere funzioni algebriche dei coefficienti di (8.1). Queste funzioni si otterranno componendo estrazioni di radici di vari indici su funzioni razionali dei coefficienti. Le operazioni più *interne*, dice Ruffini, debbono essere funzioni *razionali* dei coefficienti indicate con P', P'', P''', ecc. L'operazione successiva (eventuale) sarà un'estrazione di radice di un indice opportuno e si otterranno così espressioni del tipo

$$Q' = \alpha_1 \sqrt[p_1]{P'} \quad Q'' = \alpha_2 \sqrt[p_2]{P''} \quad Q''' = \alpha_3 \sqrt[p_3]{P'''} \ldots$$

dove $\alpha_1^{p_1} = 1$, $\alpha_2^{p_2} = 1$, $\alpha_3^{p_3} = 1$, ecc. Ora si formino tutte le possibili espressioni razionali con le varie $P^{(\cdot)}$ e $Q^{(\cdot)}$ che si indicheranno con F_1', F_1'', F_1''', ecc. di cui poi si potranno eventualmente formare ulteriori radici ottenendo

$$R' = \beta_1 \sqrt[q_1]{F_1'} \quad R'' = \beta_2 \sqrt[q_2]{F_1''} \quad R''' = \beta_3 \sqrt[q_3]{F_1'''}, ...$$

dove ora $\beta_1^{q_1} = 1$, $\beta_2^{q_2} = 1$, $\beta_3^{q_3} = 1$, ecc. Si formano poi le funzioni algebriche razionali F_2 nelle varie P, Q, R e si ripete il procedimento che, se la formula esiste, dovrà arrestarsi in un numero finito di passi. In definitiva, la formula risolutiva dovrà potersi esprimere come

$$x = G(P', \cdots, Q', \cdots, R' \cdots)$$

dove, a patto di cambiare la scelta delle radici dell'unità α_i e β_i presenti, si potranno ottenere tutte le radici di (8.1). Fatta una scelta in modo da avere

$$x_1 = G(\overline{P}, \cdots, \overline{Q}, \cdots, \overline{R} \cdots) \tag{8.10}$$

dove $\overline{P}$, $\overline{Q}$, $\overline{R}$, ecc. sono una particolare determinazione delle P', Q', R', ecc. Ora, se $n > 4$ la formula è contraddittoria. Infatti, siccome le $P^{(\cdot)}$ dipendono dai coefficienti di (8.1), per esse valgono tutte le proprietà di invarianza contenute nei teoremi $I - III$ e dunque le Q hanno le proprietà di invarianza stabilite per le y_i negli stessi teoremi che permangono anche per le F_i, per costruzione: iterando il processo, si conclude che il secondo membro di (8.10) è invariante rispetto alle permutazioni considerate nei teoremi I-III. Al contrario, il membro di sinistra *non* soddisfa questa proprietà e ciò mostra l'impossibilità dell'esistenza della formula risolutiva algebrica per (8.1).

La critica più seria mossa alla dimostrazione di Ruffini già da Burkhardt era quella di esser partito solo da funzioni razionali delle radici dell'equazione (8.1) per costruire delle risolventi di cui tentare la soluzione, sulla scorta di quanto fatto da Lagrange. In effetti, questa limitazione andava giustificata ed il merito di Abel fu quello di colmare questa lacuna dimostrando il seguente teorema ([4], p. 75), noto come Lemma di Abel.

Teorema. *Se un'equazione è risolubile algebricamente, è sempre possibile dare alla radice una forma tale che tutte le funzioni algebriche di cui essa è composta si possono esprimere tramite funzioni razionali delle radici dell'equazione proposta.*

Per la dimostrazione di questo teorema rimando a [12]. Dunque, anche la dimostrazione finale di Ruffini contiene un punto debole, colmato da Abel. Resta comunque a Ruffini il merito di aver affrontato un argomento spinoso con grande determinazione e di aver gettato le basi per la teoria dei gruppi.

Bibliografia

[1] J.L. Lagrange: Réflexions sur la résolution algébrique des équations, *Nouveaux Mém. de l'Acad. des Sciences et Belles-Lettres de Berlin*, **1**, 134–215, (1770); **2**, 138-253, (1771). In *Œuvers Complètes*, vol. 3, J.A. Serret, Ed., Gauthier-Villars, Paris, (1869), 205-421.

[2] C.F. Gauss: *Demonstratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse*; in *Gauss Werke*, vol. 3, Göttingen, (1866), 1-30.

[3] P. Ruffini, *Teoria generale delle Equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto.* Bologna, Stamperia di S. Tommaso d'Aquino, (1799). In *Opere Matematiche di Paolo Ruffini* a cura di E. Bortolotti, vol. 1, pp. 1–324, Cremonese, Roma, (1953).

[4] N. H. Abel: Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré. In *Œuvres complètes de Niels Henrik Abel*, Nouvelle Édition publiée aux frais de l' État Norvegien par MM. L. Sylow et S. Lie, Gröndahl, Christiania, 1881, Tome I, pp.66-94.≡ Beweis der Unmöglichkeit algebraische Gleichungen höheren Graden als dem vierten allgemein aufzulösen. *J. für die reine und angew. Math. (Crelle)*, **1**, 65–84, (1826).

[5] H. Burkhardt: Die Anfänge der Gruppentheorie und Paolo Ruffini. *Abhand. zur Geschichte der Mathematik* suppl. a *Zeitschr. für Math. und Phys.*, **37**, 119-159, (1892). Trad. it. di E. Pascal: Paolo Ruffini e i primordii della teoria dei gruppi, *Annali Mat. Pura ed Appl.*, **22** (S.2), (1892), 175-212.

[6] P. Ruffini: Della soluzione delle equazioni algebriche determinate particolari di grado superiore al quarto. *Mem. Soc. It. Scienze*, **9**, 444-526, (1802). In *Opere Matematiche di Paolo Ruffini* a cura di E. Bortolotti, vol. 1, pp. 345-406, Cremonese, Roma, (1953).

[7] P. Ruffini: Della insolubilità delle equazioni algebriche generali di grado superiore al quarto. *Mem. Soc. It. Scienze*, **10**, 410-470, (1803). In *Opere Matematiche di Paolo Ruffini* a cura di E. Bortolotti, vol. 2, pp. 1–50, Cremonese, Roma, (1953).

[8] G. Malfatti: Dubbi proposti al socio Paolo Ruffini sulla sua dimostrazione *Della impossibilità di risolvere le equazioni superiori al quarto grado. Mem. Soc. It. Scienze*, **11**, 579-607, (1804).

[9] P. Ruffini: Risposta di P. Ruffini ai dubbi propostigli dal socio Gian-Francesco Malfatti: *Sopra la insolubilità algebrica dell'equazioni di grado superiore al quarto. Mem. Soc. It. Scienze*, **12**, 213–267, (1805). In *Opere Matematiche di Paolo Ruffini* a cura di E. Bortolotti, vol. 2, pp. 53–90, Cremonese, Roma, (1953).

[10] P. Ruffini: Della insolubilità delle equazioni algebriche generali di grado superiore al 4°, qualunque metodo si adoperi, algebrico esso sia o trascendente. *Mem. Istit. Naz. Ital. Cl. Scienze Fis. Mat.*, **1**, 433-450, (1806). In *Opere Matematiche di Paolo Ruffini* a cura di E. Bortolotti, vol. 2, pp. 145–154, Cremonese, Roma, (1953).

[11] P. Ruffini: *Riflessioni intorno alla soluzione delle equazioni algebriche generali.* Modena, (1813). In *Opere Matematiche di Paolo Ruffini* a cura di E. Bortolotti, vol. 2, pp. 155-268, Cremonese, Roma, (1953).

[12] S. Maracchia: *Storia dell'Algebra.* Liguori, Napoli, (2005).